STATE OF ALABAMA

Information Technology Guideline

Guideline 660-02G3: Midrange Systems Security

1. INTRODUCTION:

The AS/400 midrange, formally renamed the "IBM iSeries," is a versatile all-purpose server capable of replacing PC servers and Web servers in distributed networks and supporting Web applications, data warehousing, Java application development, and e-commerce serving.

AS/400 systems use several protocols and services (including IP filtering, Network Address Translation, Virtual Private Networking, Proxy server, Secure Sockets Layer, DNS server, and Mail relay) to provide security services for these applications.

2. OBJECTIVE:

Establish a baseline security configuration for IBM midrange server equipment owned and/or operated by the State of Alabama.

3. SCOPE:

These guidelines apply to State of Alabama IBM iSeries (AS/400) midrange systems, hereafter referred to as “midrange systems.”

4. GUIDELINES:

4.1 GENERAL SECURITY REQUIREMENTS

Midrange systems shall comply with all applicable State IT Policies and Standards including but not limited to those pertaining to physical security, password usage, system access, remote access, risk and vulnerability management, backup and recovery, and information protection.

Midrange systems security controls shall be fully documented in system security plans. Plans shall be reviewed in accordance with applicable requirements.

4.2 MIDRANGE SYSTEM CONFIGURATION GUIDELINES

The State of Alabama recognizes the guidance published in the IBM Redbooks as best security practices for IBM iSeries (AS/400) system-specific configuration. IBM guidance is available for download at: http://www.redbooks.ibm.com/

The Redbook, “AS/400 Internet Security Scenarios, A Practical Approach,” explores all the native network security features available on the AS/400 system and describes their use through practical examples. It is designed to meet the needs of network administrators, consultants, and AS/400 specialists who plan to design, implement, and configure AS/400 networks connected to the Internet.

Download this Redbook at: http://www.redbooks.ibm.com/redbooks/pdfs/sg245954.pdf.

IBM publication SC41-5300: "Tips and Tools for Securing Your iSeries," provides a set of practical suggestions for using the security features of the iSeries and for establishing operating procedures that are security-conscious. The recommendations in this publication apply to an installation with average security requirements and exposures. This information does not provide a complete description of the available iSeries security features. To read about additional options or find more complete background information, consult the publications that are described in Chapter 18, "Related Information."

To view or download this IBM publication, go to:
http://publib.boulder.ibm.com/iseries/v5r2/ic2924/books/c4153006.pdf.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 660-02: System Security
http://isd.alabama.gov/policy/Policy_660-02_System_Security.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Information Technology Standard 620-03S1: Authentication-Passwords
http://isd.alabama.gov/policy/Standard_620-03S1_Authentication-Passwords.pdf

Information Technology Standard 640-02S1: Virtual Private Networks
http://isd.alabama.gov/policy/Standard_640-02S2_Virtual_Private_Networks.pdf

Information Technology Standard 650-01S1: Physical Security
http://isd.alabama.gov/policy/Standard_650-01S1_Physical_Security.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY

Version	Release Date	Comments
Original	1/30/2008	